Department of Homeland Security
IAIP Directorate
Daily Open Source Infrastructure Report
for 06 June 2005

Current Nationwide Threat Level is
ELEVATED
Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- Vnunet reports that in an unusual move phishers have targeted the membership scheme for Hilton Hotels rather than a traditional banking or auction site. (See item 4)
- The Washington Post reports a new federal rule requires all businesses and individuals to destroy private consumer information obtained from credit bureaus and other information providers used to determine whether to grant credit, hire employees, or rent an apartment. (See item 7)
- CNN reports a Virgin Atlantic flight from London to New York City was diverted to Nova Scotia on Friday, after sending out a hijack signal in what the airline and government officials called a false alarm. (See item 11)

DHS/IAIP Update *Fast Jump*

Production Industries: Energy; Chemical Industry and Hazardous Materials; Defense Industrial Base
Service Industries: Banking and Finance; Transportation and Border Security; Postal and Shipping
Sustenance and Health: Agriculture; Food; Water; Public Health
Federal and State: Government; Emergency Services
IT and Cyber: Information Technology and Telecommunications; Internet Alert Dashboard
Other: Commercial Facilities/Real Estate, Monument &Icons; General; DHS/IAIP Products &Contact Information

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *June 03, MSNBC* — **Transmission bottlenecks create vulnerability to blackouts.** California and federal energy officials repeated warnings Thursday, June 2, that the electricity system in southern California will be put to the test this summer, especially with long−range forecasts calling for hotter−than−normal temperatures. While most of the rest of the country should have adequate supplies, ongoing transmission bottlenecks continue to leave some regions of the U.S.

vulnerable to blackouts or sharp rate increases. Nationwide, demand for electricity is expected to rise by nearly six percent this summer, but generating capacity has kept up. So, most parts of the country will be okay. However, the availability of electrical power, and the price paid for it, depends heavily on location. Despite strong investment in new generating capacity in the past few years, the nation's power grid is still a patchwork of smaller markets based on regional power lines that were never designed to move electricity coast−to−coast. While power generating companies compete to sell power based on market prices set by supply and demand, most transmission lines are still regulated monopolies with a set rate of return, providing owners little financial incentive to invest in expanding capacity. If the capacity of those lines doesn't keep up with demand, pockets of the country can become overloaded.
Source: http://www.msnbc.msn.com/id/8063259/

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

2. *June 03, Reuters* — **L−3 to buy Titan.** Defense contractor L−3 Communications Holdings Inc. on Friday, June 3, said it would buy Titan Corp. for about $2 billion, expanding its reach in defense−intelligence services. The deal is the largest yet by acquisition−hungry L−3, which has grown into one of the leading U.S. defense technology firms with dozens of deals since its formation in 1997. New York−based L−3, which makes secure communications systems, chiefly for the U.S. military, hopes the deal will capitalize on the Pentagon's increased emphasis on networks and information technology. Titan, with 12,000 employees, disseminates top−secret information for the U.S. armed forces and intelligence agencies, which should help L−3 to bid on classified programs it otherwise would have difficulty winning, L−3 Chief Executive Frank Lanza said. "They (Titan) have 5,000 people −− almost half the company −− with special or top−secret clearances," he said. "That's an asset you can't price because it takes about two years to get somebody cleared."
Source: http://www.nytimes.com/reuters/business/business−arms−titan. html?

[Return to top]

Banking and Finance Sector

3. *June 04, The Korea Herald* — **Internet banking system hacked in Korea.** Seoul, Korea police on Friday, June 3, sought arrest warrants for two people on charges of hacking into an online banking system and stealing money. The case, the first of its kind in Korea, has caused widespread alarm over the security of popular Internet banking services. The government estimates online banking subscribers totaled 23 million people, about half of the population, as of April. Another two men were booked without detention for allegedly opening a bank account to which the suspects transmitted the money. The investigators said the two high school

dropouts withdrew money from a woman's account May 5 using hacking software that is easily available on Internet file−sharing services. One of the two accused posted on Internet community sites a message that carries the hacking software. The software was downloaded onto the victim's computer without her knowledge when she clicked on the message, police said. The hacking program electronically spies on the user's computer, capturing passwords and security code numbers.
Source: http://www.koreaherald.co.kr/SITE/data/html_dir/2005/06/04/2 00506040007.asp

4. *June 03, Vnunet (UK)* — **Hilton customers targeted by phishers.** In an unusual move, phishers have targeted the membership scheme for Hilton Hotels rather than a traditional banking or auction site. Professional−looking e−mails have been spammed out over the last few days asking members of the Hilton Honors scheme to re−register their details. Credit card details are also requested by the site, which is hosted in Romania. "It's the first time the Hilton has been targeted," said Mark Murtagh, technical director at Web−filtering company Websense. "People have got wiser about bank phishing and this indicates a new approach. I predict we'll see airlines, car−rental companies and other commercial concerns attacked as phishers look for alternative ways to get bank details."
Source: http://www.vnunet.com/vnunet/news/2137481/hilton−customers−t argeted−phishers

5. *June 03, Reuters* — **Technical problems hit another trading exchange.** Foreign exchange futures trading on the Chicago Mercantile Exchange's Globex electronic platform was halted on Friday, June 3, after a technical problem affected the system. Technical teams at the largest U.S. futures exchange later resolved the glitch that involved some Globex users being unable to enter or cancel currency orders, officials at the exchange said. Trading in the Japanese yen, Canadian dollar, Mexican peso, British pound, Swiss franc and EuroFX futures on Globex was shut by the problem.
Source: http://www.reuters.com/newsArticle.jhtml?type=topNews&storyI D=8691957

6. *June 02, ComputerWorld* — **Pharming attacks are soaring at an alarming rate, security experts say.** Hackers today are committing fraud at alarming rates, using sophisticated, multilayered pharming botnets. Oliver Friedrichs, security manager at Symantec Corp.'s security response center, said the increase in pharming attacks has produced a steep rise in cybercrime statistics. The company's DeepSight global Internet sensor network recorded a 360% increase in phishing or pharming e−mails during the last half of 2004. Phishers are taking advantage of drive−by installations, Friedrichs said, injecting malware into some of the vulnerabilities identified in Internet Explorer, Mozilla and Firefox browsers. The drive−by browser exploits place the infected machines into remote−controlled zombie botnets. Dan Hubbard, director of research at Websense Inc., said the "profit motive for phishing is very sizable. The hit rate is high, and the financial returns are quite good" as phishers develop more−sophisticated, "all−in−one" payloads that can proxy a server with a fake Website, log keystrokes and redirect traffic. Pharming attacks are the most ominous, said Scott Chasin, chief technology officer at MX Logic. Pharming "shows a weakness in the infrastructure of the Internet and an inability to protect the application layer," Chasin said.
Source: http://www.computerworld.com/securitytopics/security/cybercr ime/story/0,10801,102179,00.html

7.

June 02, Washington Post — **Rule requires destruction of consumer data.** A new federal rule that took effect on Wednesday, June 1, requires all businesses and individuals to destroy private consumer information obtained from credit bureaus and other information providers in determining whether to grant credit, hire employees or rent an apartment. Issued under orders from Congress, which was trying to crack down on identity theft, the Federal Trade Commission's new rule requires that personal information be burned, pulverized, shredded or destroyed in such a way that the information cannot be read or reconstructed. The rule also applies to electronic files, which must be erased or destroyed, and covers credit report data, credit scores, employment histories, insurance claims, check−writing histories, residential or tenant history and medical information.
Federal Trade Commission information on new rule:
http://www.ftc.gov/opa/2005/06/disposal.htm
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/06/01/AR2005060101940.html

8. *June 02, UPI* — **Meth addicts top list of identity thieves.** Police in Pierce County, WA, have found a 90−percent correlation between identity−theft cases and methamphetamine users. "The thing that is somewhat unique to identity theft is that it requires an almost absurd amount of hours and focus, which methamphetamine users have in abundance," said Mark Lindquist, team chief of the drug unit with the county prosecuting attorney. "We've seen methamphetamine users putting together papers that have been through shredders," said Lindquist. The wave of identity theft sweeping the area has prompted state and federal lawmakers to seek an investigation into its relationship to meth addiction.
Source: http://washingtontimes.com/upi−breaking/20050602−121619−1786 r.htm

[Return to top]

Transportation and Border Security Sector

9. *June 05, Washington Post* — **Efforts to repair aging system compound Metro's problems.** Washington, DC's world−class subway system, which for three decades has shaped the metropolitan region and delivered thousands of commuters to work on time, has fallen into a decline −− and mismanagement has been a key factor, records show. Trains break down 64 percent more often than they did three years ago, and the number of daily delays has nearly doubled since 2000. Although the vast majority of trains are on time, more than 14,400 subway riders a day are inconvenienced by a delay or a mechanical problem that forces them off broken trains. Metro officials have spent nearly $1 billion in recent years to turn around the nation's second busiest subway system, but internal records show that the projects have created new problems. The public invested more than $10 billion to build the subway. As its lines have spread across Washington and its suburbs, the system has fueled population growth, revitalized neighborhoods and stitched together a diverse region. People increasingly depend on it; since 2000, ridership is up 18 percent to nearly 660,000 passengers daily. Christened in 1976 as "America's subway," Metro created cathedral stations lauded by architects and built a technically challenging, 106−mile subway with few construction problems. And on September 11, 2001, it proved critical to evacuating Washington.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/06/04/AR2005060400350.html?sub=AR

10. *June 03, Baltimore Sun (MD)* — **New X−ray machine increases Maryland port's security.** With fears persisting that seaports are among the most vulnerable avenues for dangerous weapons to enter the country, and growing criticism of efforts to protect the borders, the port of Baltimore highlighted on Thursday, June 2, a piece of equipment that experts say can help. A powerful X−ray machine, called the Eagle, that can see through a foot of steel, bought by U.S. Customs and Border Protection for $6 million 18 months ago and brought to Baltimore in January, can scan up to 140 cargo containers a day at the state's marine terminals. Now between the new X−ray machine and an older, less powerful gamma ray machine more common at U.S. ports, officials are able to scan 14 percent of the containers that sail into the Baltimore port a year, about twice the national average. The Eagle is a 42−foot−long, 21−foot−high behemoth shaped like an upside−down U that slowly rolls on rubber tires over 20−foot and 40−foot metal containers on the pier. It can scan a 20−foot box in 30 seconds. Ships must notify Customs and the Coast Guard when they are ready to leave a foreign port or arrive in a U.S. port and provide information on crews and cargo.
Source: http://www.baltimoresun.com/news/custom/attack/bal−bz.xray03jun03,1,5166122.story?coll=bal−home−headlines&ctrack=1&cset= true

11. *June 03, CNN* — **London to New York flight diverted after false alarm.** A Virgin Atlantic flight from London, England, to New York City was diverted to Nova Scotia, Canada, on Friday, June 3, after sending out a hijack signal in what the airline and government officials called a "false alarm." Flight 045, an Airbus A340−600, with nearly 300 people on board, began sending a hijack signal mid−flight. Officials in Britain and the United States spoke with personnel onboard, who reported no problems with the flight. The plane was diverted to Halifax International Airport. Canadian F−18 fighter jets were sent to accompany the flight, a standard procedure when a hijack alert is sounded, said Gina Connell, spokesperson for Halifax International Airport. The fighter jets did not land in Halifax, but continued to a nearby air force base, she said. Passengers were "kept fully informed," Virgin Atlantic said in a statement. Virgin Atlantic spokesperson Brooke Lawer told CNN, "This was a false alarm. The transponder sent a false alert. We've been in communication with the captain who said everything is under control." An official with the British Aviation Authority also said it seemed the signal was sent out due to a mechanical error. FBI spokesperson Jim Margolin said controllers at New York's JFK International Airport tower reached the pilot on the plane, who told them, "We're not being hijacked. Everything is A−OK."
Source: http://www.cnn.com/2005/TRAVEL/06/03/flight.diverted/index.h tml

12. *June 03, Department of Homeland Security* — **Nation's busiest seaports to have complete radiation detection coverage.** Department of Homeland Security (DHS) Secretary Michael Chertoff on Friday, June 3, announced that the nation's busiest seaports −− Los Angeles/Long Beach, CA −− will have complete Radiation Portal Monitor (RPM) coverage by year's end. Three terminal locations, at Piers 400, 300 and Trans Pacific, within the Port of Los Angeles are scheduled to go on−line by the end of June. A total of ninety RPMs, which will screen all international container traffic and vehicles exiting the facility for nuclear materials or hidden sources of radiation, will be operational by December 2005. RPMs are detection devices that provide U.S. Customs & Border Protection (CBP) officers with a passive, non−intrusive means to screen containers, vessels or vehicles for the presence of nuclear and radiological materials. These systems do not emit radiation but are capable of detecting various types of radiation

emanating from nuclear devices, dirty bombs, special nuclear materials, natural sources, and isotopes commonly used in medicine and industry. The LA/Long Beach Seaports receive approximately 44 percent of all sea cargo destined for the United States. More than 4.3 million foreign cargo containers arrived at the LA/Long Beach Seaports last year −− an average of one container every seven seconds.
Source: http://www.dhs.gov/dhspublic/display?content=4530

13. *June 03, USA TODAY* — **Hawaiian leads U.S. carriers in on−time ratings.** Hawaiian Airlines officially emerged from bankruptcy protection on Wednesday, June 2, and then on Thursday, June 3, the carrier took the top spot on−time arrival rates when the Bureau of Transportation Statistics (BTS) released its April numbers. Buoyed by good weather on most of the routes it flies, 95.6% of Hawaiian's flights arrived on time in April, the last month for which statistics are available. Discount carrier ATA placed second in the monthly ratings with 89% of its April flights arriving on time. SkyWest, a commuter affiliate that operates flights for Continental, Delta and United, finished third with an on−time rating of 87.6%. At the other end of the spectrum, Alaska Airlines and JetBlue had the worst on−time ratings of the 19 large U.S. carriers that report to the BTS. Just 77% of those airlines' April flights arrived on time. Delta regional affiliate Atlantic Southeast had the third−worst on−time rating (77.3%).
Department of Transportation BTS Ratings: http://www.dot.gov/affairs/dot8505.htm
Source: http://www.usatoday.com/travel/news/2005−06−03−ontime−hawaii_an_x.htm

[Return to top]

Postal and Shipping Sector

14. *June 03, WAVY−TV (VA)* — **Legionnaires' disease strikes two Norfolk postal workers.** Health officials are investigating after two workers at the main Norfolk, VA, postal facility recently contracted Legionnaires' disease. Officials say the two employees worked the same shift, and were both manual mail processors working in the same area. That area of the postal facility has been sealed off and a spokesperson says all the air vents in the building are being tested. Results should be known early next week. The post office remains open to the public. Postal authorities found out about the two employees' condition Wednesday, June 1, and notified other facility workers. Infection comes when humans breathe the mist that comes from a water source like an air conditioning system, hot tub, or shower that has been contaminated with the Legionella bacteria. Legionellosis is a bacterial infection that can cause a variety of illnesses. Some infected individuals may experience fever and muscle aches while others can develop flu−like symptoms. The more serious form of infection characterized by pneumonia is known as Legionnaires' disease. Legionnaires' Disease is treatable with antibiotics and does not generally pose a threat to the public.
Source: http://www.wavy.com/Global/story.asp?S=3422690

[Return to top]

Agriculture Sector

15.

June 03, Capital Press (OR) — **Emergency vesicular stomatitis rule issued.** The Washington State Department of Agriculture has issued an emergency rule governing the movement of livestock from states where vesicular stomatitis (VS) has been diagnosed. Horses, cattle, swine, goats, and sheep are prohibited from entering Washington state if they come from within 10 miles of where VS has been diagnosed within the past 30 days, according to the emergency rule. Livestock entering from a state where VS has been diagnosed within the past 30 days must have an import permit and an interstate health certificate from an accredited veterinarian. This spring, VS has been diagnosed in New Mexico, Arizona, and Texas. Vesicular stomatitis spreads relatively easily. Once introduced into a herd, VS is transmitted by contact or exposure to saliva or fluid from ruptured lesions. Affected animals have blisters in the mouth, on the udder or on feet. Excessive salivation often occurs, and complications can include secondary bacterial infections, malaise, and mastitis.
Source: http://www.capitalpress.info/main.asp?SectionID=67&SubSectionID=782&ArticleID=17614&TM=29005.88

16. *June 03, Pennsylvania Department of Agriculture* — **Pennsylvania announces plum pox detection.** Pennsylvania Agriculture Secretary Dennis Wolff Friday, June 3, announced the first detection of Plum Pox Virus for 2005. Plum Pox is a virus that severely decreases fruit production. “Our testing laboratory has confirmed the presence of Plum Pox Virus in a single tree in a four acre block of commercial peaches,” Wolff indicated. “The trees are in the already quarantined portion of Menallen Township, Adams County.” Wolff added that the Department will follow its standard procedure of establishing a 500−meter radius buffer zone around the infected block and ordering removal and destruction of all virus−susceptible stone fruit trees in the buffer zone. Two additional blocks of peach trees totaling about 10 acres will also have to be removed as a result of this detection. Only one commercial grower has been impacted by this find.
Source: http://www.agriculture.state.pa.us/agriculture/cwp/view.asp? Q=134795&A=390

[Return to top]

Food Sector

Nothing to report.
[Return to top]

Water Sector

17. *June 03, The Monitor (TX)* — **Texas water plant determined to protect area water supply.** The municipal water plant is not one of the places people can freely visit if they want to contribute to the city’s tourism dollars. But it is one of the locations Edinburg, TX leaders want to keep safe in an ongoing effort at fighting terrorism on the home front. The city, along with others in Texas, have access to training and programs enabling municipal workers to better understand what must be done to enhance safety and security to keep its water supply safe. The plant has a 6−foot−tall chain link fence topped by barbed wire. Barriers will be used to block drivers, but special access will be granted to people living on a closed road beside the plant. The Department of Homeland Security (DHS) set forth requirements in its 2002 Bioterrorism

Act mandating what utility plant owners had to do to keep water and sewage supplies safe from terrorists. DHS has required utility plant owners to perform a vulnerability assessment plan that must be periodically updated to determine what security aspects had to be improved. The report is not public record because it is protected under the Texas Homeland Security Act, according to the Texas Attorney General's Office in Austin.
Source: http://www.themonitor.com/SiteProcessor.cfm?Template=/GlobalTemplates/Details.cfm&StoryID=7524&Section=Valley

18. *June 02, Associated Press* — **Wet winter eases southwest drought.** An unusually wet winter has led to the easing of the drought across much of the Southwest, officials said Thursday, June 2. With runoff from heavy snow feeding reservoirs, conditions in most of the region have been upgraded from drought to abnormally dry, officials said. "We had this great winter, with lots of snow and rain," said Michael Hayes, climate impacts specialist at the University of Nebraska−Lincoln's National Drought Mitigation Center. "All of the Southwest has recovered significantly from the drought conditions. Parts of the Southwest have recovered completely." However, more rain is needed to fill regional reservoirs. Water levels remains below capacity at Lake Powell, Lake Mead and at most reservoirs in New Mexico. Varying degrees of drought continue elsewhere in the West and Southwest, including in northeastern Arizona and northwestern New Mexico.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/06/02/AR2005060201652.html

[Return to top]

Public Health Sector

19. *June 02, Associated Press* — **Whooping cough booster shot appears safe.** An experimental booster shot designed to protect adults and adolescents from whooping cough proved safe and effective in a study released Thursday, June 2, offering a vital new tool for fighting a dangerous resurgence of the disease over the past few years. The vaccine, developed by Sanofi Pasteur and already widely given to teenagers in Canada, appears likely to win U.S. government approval later this month. The vaccine is needed "to prevent the disease in teenagers and adults themselves and, secondly, take away their ability to be contagious," said Michael E. Pichichero, a professor at the University of Rochester Medical Center who has headed clinical trials into the vaccine since 2001. "We're trying to stop an epidemic." Cases of whooping cough, an ancient scourge that effective vaccination of babies and toddlers was meant to wipe out, have quadrupled in the U.S. over the past three years to 18,957 cases in 2004. It turns out the vaccine that babies get starts wearing off by adolescence. The study indicated that the booster shot should be at least 83 percent effective at preventing severe illness in adults and adolescents, though no one yet knows how long the renewed immunity will last.
Vaccine study: http://jama.ama−assn.org/cgi/content/full/293.24.3003v1
Source: http://news.yahoo.com/s/ap/20050603/ap_on_he_me/whooping_cough_vaccine;_ylt=AiqiGlLGAsQEhgEPdbeqLUdZ24cA;_ylu=X3oDMTBiMW04NW9mBHNlYwMlJVRPUCUl

20. *June 02, National Institute of Allergy and Infectious Diseases* — **Variant prion causes infection but no symptoms.** Abnormal prion proteins are little understood disease agents

involved in causing brain−wasting diseases such as Creutzfeldt−Jacob disease in humans, mad cow disease in cattle, and chronic wasting disease in deer. New research suggests that a variant form of abnormal prion −− one lacking an “anchor” into the cell membrane—may be unable to signal cells to start the lethal disease process, according to scientists at the Rocky Mountain Laboratories, part of the National Institute of Allergy and Infectious Diseases (NIAID). “This work provides novel insights into how prion and other neurodegenerative diseases develop and it provides clues as to how we might delay or even prevent such diseases by preventing certain cellular interactions,” notes NIAID Director Anthony S. Fauci. The research team exposed two groups of mice to different strains of the agent that causes scrapie, a brain−wasting disease of sheep. Within 150 days of being inoculated with the natural form of scrapie prion protein, all 70 mice in the control group showed visible signs of infection. In contrast, the scientists observed 128 transgenic mice −− those engineered to produce prion protein without a glycophosphoinositol cell membrane anchor −− for 500 days and saw no signs of scrapie disease. Microscopic examinations; however, confirmed that they produced an abnormal form of prion protein and had brain lesions.
Source: http://www2.niaid.nih.gov/newsroom/Releases/variant_protein. htm

21. *June 02, Howard Hughes Medical Institute* — **Virus uses tiny RNA to evade the immune system.** In the latest version of the hide−and−seek game between pathogens and the hosts they infect, researchers have found that a virus appears to cloak itself with a recently discovered gene silencing device to evade detection and destruction by immune cells. The report by Howard Hughes Medical Institute (HHMI) researchers may be the first to show how a virus uses the gene silencing machinery for its own infectious purposes. In people, plants, and worms, hundreds of tiny RNA molecules can silence specific genes by interfering with larger messenger RNAs (mRNAs). That interference prevents mRNAs from making proteins. Scientists do not know which genes are hushed by the micro RNAs in people, but the new study bolsters growing evidence that the tiny molecules can play important roles not only in normal human cells but in infected cells as well. “A popular notion is that the whole system of generating small RNAs was designed to be a defense by cells against viruses. Our study shows that a virus can also adapt it to evade the immune response,” said Don Ganem, HHMI investigator.
Source: http://www.hhmi.org/news/ganem3.html

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

22. *June 03, Associated Press* — **Fort Lauderdale prepares for massive security operation at Convention Center.** When the Organization of American States General Assembly begins meets June 5−7, at the Broward County Convention Center in Fort Lauderdale, representatives of more than 26 local, state and federal authorities will be running a massive security operation

in Fort Lauderdale. Their challenge: Find the right balance between keeping the public safe and not stifling the rights of protesters, who could number in the thousands. "We anticipate a peaceful weekend," said Fort Lauderdale police Sgt. Andy Pallen. Law enforcement agencies have conducted field training, developed detailed strategies and rehearsed countless "What if?" scenarios so that nothing −− be it a terrorist attack or violent protests−− takes them by surprise. The OAS security operation will be one of the biggest in the United States this year, on par with events such as the Super Bowl and the United Nations General Assembly in New York, said Ed Moreno, special agent in charge at the State Department's Diplomatic Security Service field office in Miami.
Source: http://www.securityinfowatch.com/article/article.jsp?siteSec tion=306&id=4253

23. *June 03, Hattiesburg American (MS)* — **Mock anthrax attack prepares hospital for real thing.** Decontamination specialists utilize pressurized hoses Thursday, June 2, to wash away the fictional anthrax that covered nurse Eric Peters under a Hazmat tent at Forrest General Hospital in Hattiesburg, MS, during a simulated anthrax attack. Hours after a mysterious aerosol spray filled the air at a junior college graduation on Thursday, about 150 people with flu−like symptoms flooded Forrest General Hospital desperately looking for help. But the patients didn't have the flu. They were victims of an anthrax attack −− actually, a mock anthrax attack designed to teach hospital volunteers what they should do in the event of an actual biological or chemical terrorist strike. Mack Strider, emergency response coordinator for the Mississippi Department of Health, said numerous trains traveling through the state carry chlorine and other hazardous chemicals. In most cases, Strider said, victims will be decontaminated once at the site of accidents or attacks and then again at Forrest General. He said that ensures no toxins enter the hospital. "You can't let anything get into the hospital," Strider said. "If something does, you really have some problems."
Source: http://www.hattiesburgamerican.com/apps/pbcs.dll/article?AID =/20050603/NEWS01/506030304/1002

[Return to top]

Information Technology and Telecommunications Sector

24. *June 03, Associated Press* — **Microsoft says MSN Website hacked in South Korea.** Microsoft acknowledged Thursday, June 2, that hackers booby−trapped its popular MSN Website in South Korea to try to steal passwords from visitors. The company said it was unclear how many Internet users might have been victimized. Microsoft said it cleaned the Website, http://www.msn.co.kr and removed the dangerous software code that unknown hackers had added earlier this week. A spokesperson, Adam Sohn, said Microsoft was confident its English−language Websites were not vulnerable to the same type of attack. The Korean site, unlike U.S. versions, was operated by another company Microsoft did not identify. Microsoft's own experts and Korean police authorities were investigating, but Microsoft believes the computers were vulnerable because operators failed to apply necessary software patches, said Sohn, an MSN director. MSN Korea said the only site affected by the hacking was the MSN Korea news site: http://news.msn.co.kr
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/06 /02/AR2005060201604.html?nav=hcmodule

25. *June 03, BBC News (UK)* — **Fake Osama bin Laden e−mail hides virus.** Users are being warned not to open junk e−mail messages claiming Osama bin Laden has been captured. The messages claim to contain pictures of the al Qaeda leader's arrest but anyone opening the attachment will fall victim to a Microsoft Windows virus. Since June 1, anti−virus companies have been catching the junk mail messages in large numbers. Anyone opening the attachments or visiting the Website will get a version of the Psyme trojan installed on their PC. The vulnerability exploited by Psyme is found in Windows 2000, 95, 98, ME, NT, XP and Windows Server 2003. Users are urged to update their version of Windows to close the loophole.
Source: http://news.bbc.co.uk/1/hi/technology/4607203.stm

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT reports a heap−based buffer overflow that affects the PHP 'pack()' function call. An attacker that has the ability to make the PHP interpreter run a malicious script may exploit this condition to execute arbitrary instructions in the context of the vulnerable process. This function allows a malicious programmer to set references to entries of a variable hash that have already been freed. This can lead to remote memory corruption and may allow them to gain access to potentially sensitive information, such as database credentials.

Current Port Attacks

Top 10 Target Ports	135 (epmap), 445 (microsoft−ds), 1026 (−−−), 1027 (icq), 1433 (ms−sql−s), 1434 (ms−sql−m), 4899 (radmin), 139 (netbios−ssn), 1028 (−−−), 25 (smtp) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

26. *June 04, St. Petersburg Times (FL)* — **Terrorism fears halt Florida port fireworks.** Last week, the Coast Guard captain responsible for Florida's Tampa Port Authority turned down a request from a downtown business group to open the waterfront for fireworks on Friday evenings from June through August. The conflict involves a long concrete wharf for cruise ships at the port. Running from behind the Channelside entertainment complex to the Florida Aquarium, the wharf is closed off to the public by a high metal fence. U.S. Customs regulations require access to the area be restricted during cruise ship calls to make sure undocumented

people and cargo don't get on or off the vessel. For the second year, the Coast Guard has agreed to fireworks displays on the Channel District waterfront for four holidays: Memorial Day and Labor Day weekends, the Fourth of July and New Year's Eve. Port Capt. Mike Farley wrote the merchants group May 23 that the weekly events would "create a repetitive and predictable diversion terrorists could exploit to mask their activities." The port authority and local law enforcement agencies provide enough extra security to make the holiday events secure, Farley said. But holding fireworks every week could "desensitize" officers and let terrorists blend in with bystanders. Cruise ships carrying upwards of 3,000 passengers and crew are considered prime terrorist targets.
Source: http://www.sptimes.com/2005/06/04/Business/Terrorism_fears_h alt_.shtml

27. *June 03, USA TODAY* — **Schools restrict use of Tasers.** Dozens of incidents in which police officers have used electric stun guns to subdue unruly students have led school officials around the U.S. to restrict the use of the devices on campus. The Taser is relatively safe compared with other objects that can transmit electricity to humans, says Vincent Amuso, associate head of electrical engineering at the Rochester Institute of Technology. What makes the Taser less harmful is the short length of time it is held against the body, he says. Some people think of electricity in terms of volts, but voltage is actually a measure of how much electricity can be moved. Schools in St. Paul, MN, and elsewhere have joined Miami−Dade, FL, in limiting stun guns. St. Paul's school board voted in May to allow officers in schools to use them on students only in life−threatening situations. In Jacksonville, FL, Sheriff John Rutherford is holding 16 town meetings on stun guns in schools to help him set a policy for the next school year. He says he is inclined to allow their use in schools — but only when lethal force is justified.
Source: http://www.usatoday.com/news/nation/2005−06−03−taser_x.htm

[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS/IAIP Products & Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures:

DHS/IAIP Daily Open Source Infrastructure Reports − The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS/IAIP Daily Open Source Infrastructure Report is available on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

Homeland Security Advisories and Information Bulletins − DHS/IAIP produces two levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is

significant, credible, timely, and that addresses cyber and/or infrastructure dimensions with possibly significant impact. Homeland Security Advisories and Information Bulletins are available on the Department of Homeland Security Website: http://www.dhs.gov/dhspublic/display?theme=70

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 983−3644 for more information.

Contact DHS/IAIP

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

DHS/IAIP Disclaimer